BAKER BOTTS L.L.P.
Wayne O. Stacy (SBN 314579)
wayne.stacy@bakerbotts.com
Sarah Guske (SBN 232467)
sarah.guske@bakerbotts.com
Jeremy J. Taylor (SBN 249075)
jeremy.taylor@bakerbotts.com
BAKER BOTTS L.L.P.
101 California Street, Suite 3600
San Francisco, California 94111
Telephone: (415) 291-6200
Facsimile: (415) 291-6300

Kurt M. Pankratz (*pro hac vice*)
kurt.pankratz@bakerbotts.com
BAKER BOTTS L.L.P.
2001 Ross Avenue
Dallas, Texas 75201-2980
Telephone: (214) 953-6584
Facsimile: (214) 661-4584

Jake W. Gallau (SBN 319656)
jake.gallau@bakerbotts.com
BAKER BOTTS L.L.P.
1001 Page Mill Road, Bldg. One, Suite 200
Palo Alto, California 94304
Telephone: (650) 739-7500
Facsimile: (650) 739-7699

Attorneys for Plaintiff
DROPBOX, INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

DROPBOX, INC.,

Plaintiff,

vs.

SYNCHRONOSS TECHNOLOGIES, INC.,

Defendant.

Case No.

PLAINTIFF'S COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

PLAINTIFF'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Dropbox, Inc. ("Dropbox" or "Plaintiff") files this complaint for patent infringement against Defendant Synchronoss Technologies, Inc. ("Synchronoss" or "Defendant") and in support thereof alleges as follows:

THE PARTIES

1. Dropbox, Inc. is a corporation organized under the laws of the State of Delaware, with a principal place of business at 333 Brannan Street, San Francisco, California.

2. On information and belief, Synchronoss Technologies, Inc. is a corporation organized under the laws of the State of Delaware, with a principal place of business at 200 Crossing Boulevard, 8th Floor, Bridgewater, New Jersey.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the Patent Laws of the United States of America, Title 35, United States Code.

4. This Court has subject-matter jurisdiction over Dropbox's claims under 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Synchronoss. Synchronoss has continuous and systematic business contact with the State of California and has committed acts of patent infringement within the Northern District of California. For example, Synchronoss's offices are located at 60 South Market Street in San Jose, California. In addition, Synchronoss regularly conducts business in California and attempts to derive benefit from residents of the State of California by offering infringing products, such as the Synchronoss Personal Cloud, in the Northern District of California.

6. Venue is proper in this judicial district under 28 U.S.C. §§ 1391 and 1400(b). Synchronoss resides in the Northern District of California, and Synchronoss has committed acts of infringement in this District and has a regular and established place of business in this District. Synchronoss conducts business from its permanent physical location located in the Northern District of California at 60 South Market Street, San Jose, California. On information and belief, at least 36 employees are employed at this Synchronoss location, including

employees responsible for engineering, marketing, customer support, and product development. As described herein, Synchronoss offers infringing products, including the Personal Cloud product in the Northern District of California.

THE PATENTS-IN-SUIT

7. U.S. Patent No. 7,567,541 ("the '541 Patent"), titled "System and Method for Personal Data Backup for Mobile Customer Premises Equipment," was issued by the United States Patent and Trademark Office ("USPTO") on Jul. 28, 2009. Dropbox is the owner by assignment of the entire right, title and interest in and to the '541 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '541 Patent is attached hereto as Exhibit A.

8. U.S. Patent No. 6,058,399 ("the '399 Patent"), titled "File Upload Synchronization," was issued by the USPTO on May 2, 2000. Dropbox is the owner by assignment of the entire right, title and interest in and to the '399 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '399 Patent is attached hereto as Exhibit B.

9. U.S. Patent No. 6,178,505 ("the '505 Patent"), titled "Secure Delivery of Information in a Network," was issued by the USPTO on Jan. 23, 2001. Dropbox is the owner by assignment of the entire right, title and interest in and to the '505 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '505 Patent is attached hereto as Exhibit C.

10. The '541 Patent, '399 Patent, and '505 Patent are referred to herein collectively as the Patents-in-Suit.

BACKGROUND OF THE DISPUTE

Dropbox Is a Pioneer in Syncing, Sharing, and Backup of User Data

11. Dropbox was founded in June 2007 by Drew Houston and Arash Ferdowsi. It launched in September 2008 as a simple way for people to access their files wherever they are and share them easily. The simplicity of the product combined with the reliability of the sync led consumers to bring Dropbox to work to empower collaboration. Over 300,000 teams have

adopted Dropbox Business, and there are over 500 million registered Dropbox users around the world.

12. Dropbox's global collaboration platform is a market leader where users create, access, and share content. Underlying Dropbox's success is its tremendous investment in research and development, including in the areas of data backup and transfer. Through these efforts, Dropbox has obtained valuable intellectual property in these areas.

Synchronoss's Infringing Cloud Products

13. Synchronoss was founded in 2000 by Stephen G. Waldis but is a relative newcomer to consumer cloud backup, launching its Personal Cloud product more than a decade later.

14. Synchronoss sells its Personal Cloud product as a white-label data backup and transfer solution to network operators or service providers, such as Verizon.

15. Synchronoss has gained momentum in the marketplace through unlawful use of the technology claimed in the Patents-in-Suit.

16. On information and belief, Synchronoss's Cloud products, including without limitation its Personal Cloud product, infringes the Patents-in-Suit, as described in more detail below.

PATENT INFRINGEMENT CLAIMS

Count I – Infringement of U.S. Patent No. 7,567,541

17. Dropbox incorporates by reference the allegations in Paragraphs 1 through 16 above.

18. The '541 Patent was filed on April 20, 2006 and claims priority to U.S. provisional application No. 60/620,543, filed October 20, 2004.

19. At the time that the '541 Patent was filed, several technological shortcomings existed that made data backup and restoration burdensome for users of mobile customer premises equipment ("CPE") such as cell phones. *See* Ex. A ('541 Patent) at 1:30–60. Those shortcomings stem from the absence of a flexible system for backing up data from one device such that it could later be easily transmitted back to the same or another device. Then-existing

methods for transferring data included manual entry of each address, contact, calendar event, etc., or the transfer of data directly from one device to another using a cradle. Manual entry bears the disadvantage of being extremely time intensive. *Id.* at 1:30–34. A specialized cradle, meanwhile, suffers from disadvantages including data backup or transfer only occurring when the user has all of the required equipment (a first device, a cradle, and, in the case of transfer, a second device) at the same physical location at the same time. *Id.* at 1:42–48. Additionally, the necessary cradles were not widely available, and transfers or backups usually needed to be performed in-store by an authorized technician. *Id.* at 1:49–52. Other general problems, not directly associated with manual entry or specialized cradles, also prevented effective data backup and transfer, including device incompatibility preventing data transfer and irreparable loss of data due to the destruction of a device. *Id.* at 1:49–56.

20. Recognizing the deficiencies associated with existing approaches to data backup and transfer, the '541 Patent describes specific and discrete implementations to flexibly back up data stored on customer premises equipment such as mobile phones. These methods were significant improvements over prior approaches to data backup in that they provided improved accessibility to users who wanted to backup or transfer data to/from their devices without professional support or the need to travel to a store with the necessary specialized cradle. Further, these methods and systems include a novel approach to data formatting that allows for the transfer of data from a device of one make, model, and ecosystem to another device of a different make, model, and ecosystem. *See, e.g., id.* at 1:56–59. This approach to formatting data also allows for the backup or transfer of only certain types of data including only that data that has changed since a previous data backup. *See, e.g., id.* at 2:11–33, 2:60–3:34.

21. The '541 Patent describes and claims a number of novel and inventive approaches to data backup. These inventive approaches are captured in independent Claims 1, 11, 17, 21, and their respective dependent claims. The claimed approaches are tied to computers and cannot be performed by a human alone. Claim 1, for example, recites "[a] method for backing up data stored on a mobile customer premises equipment" comprising "storing data at the mobile customer premises equipment;" "formatting the data . . . into fields by determining

data fields, identifying which portions of said data correspond to a respective data field, and tagging said data;" "transmitting the data with a user ID . . . to a server for storage;" "retrieving said data . . . in response to one of an expiration of time and request;" and "transmitting the data in more than one information signal and sequentially numbering each of said information signals."

22. Claim 11 recites "[a] method for backing up data stored on a mobile customer premises equipment" comprising "formatting the data at the mobile customer premises equipment into fields;" "transmitting only the changes in data which have occurred since a previous transmission;" "transmitting only the changes in the data with a user ID . . . to a server for storage, by transmitting the data in more than one information signal across the mobile network and sequentially numbering each of said information signals, in response to one of an expiration of time, request from said server, and change in status of data at said mobile customer premises equipment;" and "said server storing said data for retrieval and transmitting said data to the mobile premises equipment."

23. Claim 17, meanwhile, recites "[a] system for backing up data on a mobile customer premises equipment" comprising "a mobile customer premises equipment . . . storing data thereon, the data being formatted into fields, and selectively sending a request for the data;" and "a server in communication with said mobile customer premises equipment across a mobile network and storing said data, said mobile customer premises equipment transmitting the data with a user ID to said server in more than one information signal and sequentially numbering each of said information signals, said server storing said data for retrieval by determining data fields, identifying which portions of said data correspond to a respective data field, and tagging said data, said data being retrieved from said server in response to one of an expiration of time and requests from said mobile customer premises equipment, said server transmitting said data to said mobile customer premises equipment."

24. Claim 21, meanwhile, recites "[a] system for backing up data on a mobile customer premises equipment" comprising "a mobile customer premises equipment storing data thereon, the data being formatted into fields, and selectively transmitting said data with a user

ID;" and "a server in communication with said mobile customer premises equipment across a mobile network and storing said data for retrieval by said mobile customer premises equipment, said server storing said data in response to transmission of said data from said mobile customer premises equipment, said mobile customer premises equipment transmitting only the changes in data which have occurred since a previous transmission to said server in response to one of an expiration of time and request from said server by transmitting the change in data in more than one information signal across a mobile network, and sequentially numbering each of said information signals."

25. These claim elements, individually or in combination, are unconventional, and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, as explained previously, the claimed concepts solve problems of the prior art described in the patent and provide advantages and improvements to data backup and transfer that was unknown in the field before the invention of the '541 Patent. *See, e.g.*, Ex. A at 1:19–60, 2:11–33, 2:60–3:34. Unlike conventional approaches to data backup and transfer, the inventions described and claimed in the '541 Patent require specific formatting and transmission parameters that, when used in combination with other claim elements, improve data backup and transfer in unconventional ways. *See id.* For example, as previously described, prior to the invention of the '541 Patent, existing data backup and transfer methods included manual entry of each address, contact, calendar event, etc., or the transfer of data directly from one device to another using a cradle. *Id.* at 1:19–60. The inventions described and claimed in the '541 Patent solved these problems and improved data backup and transfer technology when implemented. *Id.* at 2:11–33, 2:60–3:34.

26. The solutions described and claimed in the '541 Patent represented a significant advance over existing approaches and were not well-known, routine, or conventional in the field at the time the application leading to the '541 Patent was filed. *See id.* at 1:19–60, 2:11–33, 2:60–3:34. During examination of the application that ultimately issued as the '541 Patent, the patent examiner at the United States Patent and Trademark Office ("USPTO") considered multiple U.S. patent documents. *See* Ex. A at Cover Page. These include references describing

solutions from Panasonic, Nokia, Sony, and NTT Docomo, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the '541 Patent.

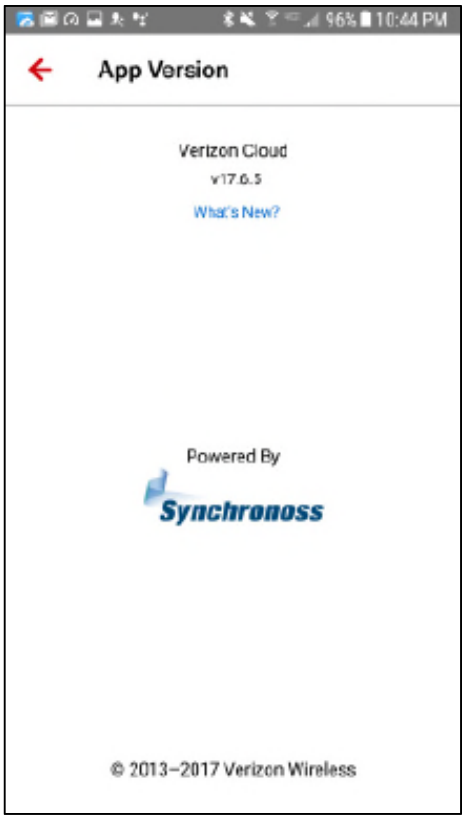
27. Synchronoss directly infringed and continues to directly infringe one or more claims of the '541 Patent, either literally or under the doctrine of equivalents, by making, using, offering to sell, and selling the Synchronoss Personal Cloud. Non-limiting examples of such infringement are provided below, based on the information currently available to Dropbox.

28. Synchronoss's Personal Cloud, for example, satisfies each and every limitation of Claim 1 of the '541 Patent.

29. Synchronoss's Personal Cloud is accessible via a mobile application, a desktop application running on a personal computer, and a website accessed using a web browser running on a personal computer.

30. Synchronoss's Personal Cloud performs a method for backing up data stored on a mobile customer premises equipment. For example, Synchronoss's Personal Cloud provides Personal Cloud to mobile network providers as a "white-label solution" for syncing, backing up, and uploading data (e.g., contacts, photographs, videos, music, documents, messages, and/or call history) stored on users mobile phones. *See* http://synchronoss.com/products/cloud/personal-cloud-solution.

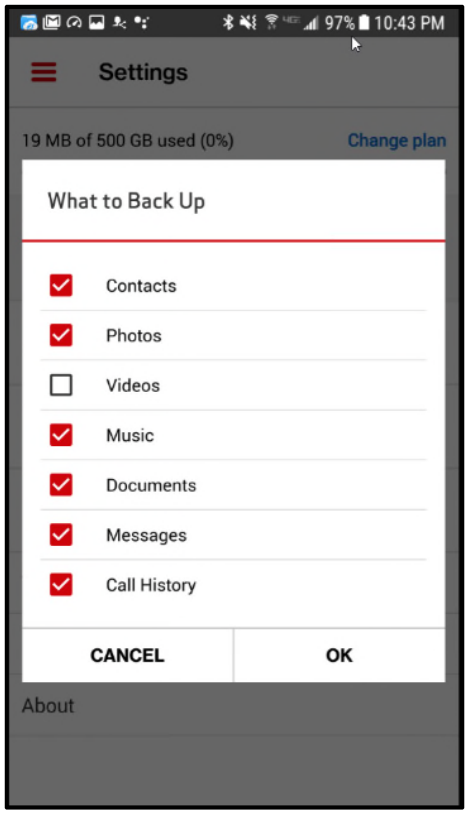
31. For example, Synchronoss provides the Synchronoss Personal Cloud product to Verizon:



Synchronoss Personal Cloud mobile application screenshot.

32. Synchronoss's Personal Cloud stores data at the mobile customer premises equipment. For example, Personal Cloud allows syncing, backing up, and uploading data (e.g., contacts, photographs, videos, music, documents, messages, and/or call history) stored at the mobile customer premises equipment. *See* http://synchronoss.com/products/cloud/personal-cloud-solution.

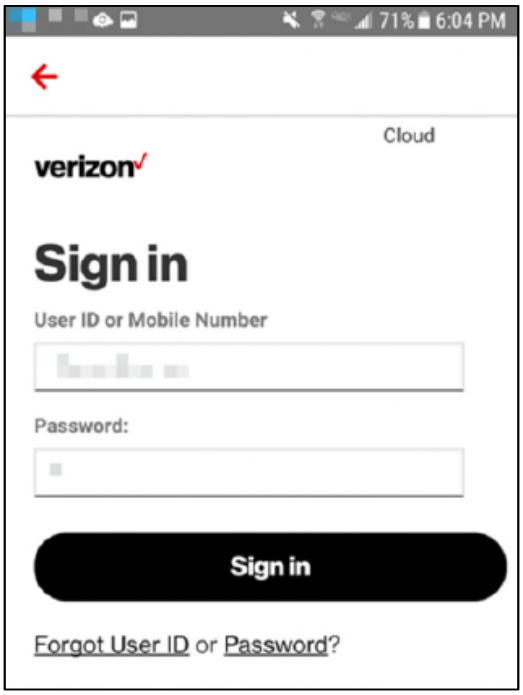
33. Synchronoss's Personal Cloud formats the data stored at the mobile customer premises equipment into fields by determining data fields, identifying which portions of said data correspond to a respective data field, and tagging said data. For example, data fields are used in the Synchronoss Personal Cloud to categorize uploaded data stored at a mobile phone. These data fields may include contacts, photographs, videos, music, documents, messages, and/or call history:



Synchronoss Personal Cloud mobile application screenshot.

34. As another example, Synchronoss's Personal Cloud formats the data stored on mobile phones into data fields specific to each type of data being backed up. Photograph data, for example, includes date, time, and geographic location data fields, and contact data includes data fields representing a contact's first name, last name, email address, physical address, phone number, and company.

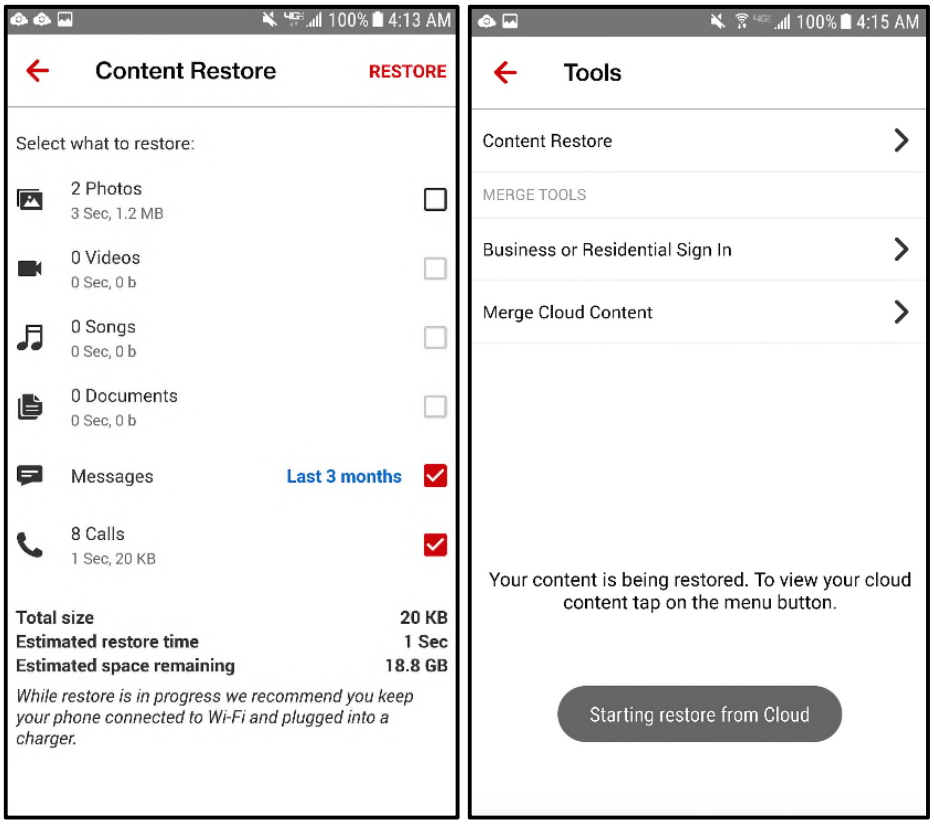
35. Synchronoss's Personal Cloud transmits the data with a user ID from the mobile customer premises equipment across a mobile network to a server for storage. For example, the user phone number or user ID is required to access the Synchronoss Personal Cloud:



Synchronoss Personal Cloud mobile application screenshot.

36. Data stored on the Synchronoss Personal Cloud is associated with the user ID or phone number used to log into the Synchronoss Personal Cloud, and on information and belief, these and/or other identifiers, including IP address, account number, device ID, or session ID, are transmitted with the data between the mobile customer premises equipment to a server.

37. Synchronoss's Personal Cloud retrieves said data from said server across a mobile network in response to one of an expiration of time and request from said mobile customer premises equipment by transmitting said data to said mobile customer premises equipment. For example, Synchronoss's Personal Cloud allows a user to request and download data (e.g., contacts, photographs, videos, music, documents, messages, and/or call history) to a mobile phone or other device from the server:



Synchronoss Personal Cloud mobile application screenshot.

38. Synchronoss's Personal Cloud transmits said data to said mobile customer premises equipment by transmitting the data in more than one information signal and sequentially numbering each of said information signals. For example, sequentially-numbered TCP/IP packets are used to transmit data between mobile phones and Synchronoss Personal Cloud servers. Wi-Fi and LTE technologies also use sequentially-numbered packets to wirelessly transmit data between mobile devices and Synchronoss Personal Cloud servers.

39. Synchronoss has been aware of the '541 Patent since at least filing and service of this complaint.

40. Synchronoss has been aware of Dropbox since at least March 27, 2015 when it filed a lawsuit against Dropbox.

41. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss investigated Dropbox's intellectual property before or during its lawsuit against Dropbox.

42. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss was aware of the '541 Patent prior to the filing of this complaint.

43. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss's infringement of the '541 Patent has been willful and deliberate.

44. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to conduct an investigation after learning of the '541 Patent.

45. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to take any remedial actions upon learning of the '541 Patent.

46. Synchronoss also indirectly infringed and continues to indirectly infringe the '541 Patent by inducing and contributing to infringement of the '541 Patent in violation of 35 U.S.C. § 271(b) and (c).

47. Synchronoss induced and continues to induce its customers and end users to infringe the '541 Patent by making, using, offering to sell, and/or selling the Synchronoss Personal Cloud. Synchronoss configures the Personal Cloud to operate in a manner that Synchronoss knows infringes the '541 Patent and encourages customers and end users to use Synchronoss's Personal Cloud in a manner that Synchronoss knows infringes the '541 Patent. For example, Synchronoss's marketing literature touts functionality of the Synchronoss Personal Cloud that falls within the scope of the above-identified claims of the '541 Patent.

48. Synchronoss contributed to and continues to contribute to the infringement of the '541 Patent by selling and offering to sell the Synchronoss Personal Cloud to network operators or service providers who incorporate the infringing Synchronoss Personal Cloud into branded cloud backup products. As described previously, Synchronoss's Personal Cloud is especially made for infringement of the '541 Patent. Synchronoss's Personal Cloud is not a staple article or commodity of commerce suitable for substantial non-infringing use. The only use of the Synchronoss Personal Cloud results in an act of direct infringement.

49. Dropbox has no adequate remedy at law for Synchronoss's acts of infringement. As a direct and proximate result of Synchronoss's acts of infringement, Dropbox has suffered and continues to suffer damages and irreparable harm. Unless Synchronoss's acts of willful

infringement are enjoined by this Court, Dropbox will continue to be damaged and irreparably harmed by Synchronoss's ongoing willful infringement.

Count II – Infringement of U.S. Patent No. 6,058,399

50. Dropbox incorporates by reference the allegations in Paragraphs 1 through 49 above.

51. The '399 Patent was filed on August 28, 1997.

52. In the mid-1990s, the options available for transferring data to websites and other service providers were limited. Options that did exist ran independently of a web browser, required manual file name input, or provided limited security. Ex. B ('399 Patent) at 1:11–27. The available file-upload methods were cumbersome, often requiring substantial computer literacy. *Id*. at 1:34–36.

53. The '399 Patent identified the need to "provide a method of uploading large amounts of data . . . [that was] more user friendly than [the existing methods]," and provided specific and discrete implementations for solving these problems. *Id.* at 1:36–39. In an improvement over prior art approaches to uploading data files, the invention described and claimed in the '399 Patent "synchroniz[es] the file upload session and the interactive session." *Id*. at 2:64–67. By associating the uploaded files with the interactive connection, more efficient and user-friendly file uploading can be achieved. *See id*. at 1:41–54. For example, using the claimed invention, "the interactive session can determine which files have been uploaded" and enable the cancelling of queued uploads through the interactive session. *Id*. at 3:1–3. A session ID can also be used to "differentiate multiple users and/or multiple sessions from a single user . . . [and to] breakdown a single session into a plurality of interactive sessions." *Id.* at 3:4–9. All these improvements granted greater usability and security to website users. *See id*. at 1:41–3:47.

54. The '399 Patent describes and claims a number of novel and inventive approaches to data uploading, including synchronizing an interactive connection and a non-interactive data transfer connection. These inventive approaches are captured in independent Claims 1, 11, 25, 32, 36, 43, 46, and their respective dependent claims. The claimed approaches are tied to computers and cannot be performed by a human alone. Claim 1, for example, recites

"creating an interactive connection;" "creating a data transfer connection;" and "generating a single session ID for the two connections, which ID associates between the two connections."

55. Claim 11 recites "creating an interactive connection between the client and the service provider;" "creating a data transfer connection between the client and the service provider;" and "automatically uploading data files from the client to the service provider, on the data transfer connection, responsive to the interactive connection."

56. Claim 25 recites "a file upload connection server," "an interactive connection server," and "a synchronizer which synchronizes the operation of respective connections formed by the file upload connection server and by the interactive connection server."

57. Claim 32 recites "a file upload connection client," "an interactive connection client," and "a client synchronizer which synchronizes the operation of respective connections formed by the file upload connection client and by the interactive connection client."

58. Claim 36 recites a "file upload monitor, which monitors the operation of a file upload server without direct communication with the file upload server;" "an interactive data generator, which generates data in a format suitable for an interactive connection server;" and "a synchronizer . . . [that] causes said interactive data generator to generate data responsive to input from said file upload monitor and which sends the generated data through the interactive connections server."

59. Claim 43 recites "uploading a list of file information for a plurality of local files to a remote server;" "generating a data display at the remote server;" and "locally displaying said data display, wherein said data display includes local data not downloaded from the remote server, responsive to said local file information."

60. Claim 46 recites "connecting from said client to said server;" "receiving information comprising a username at said client from said server;" and "uploading files from said client to said server, utilizing said information."

61. These claim elements, individually or in combination, are unconventional, and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, as explained previously, the claimed concepts solve problems of

the prior art described in the patent and provide advantages and improvements to data uploading that was unknown in the field before the invention of the '399 Patent. *See, e.g.,* Ex. B at 1:11–3:47. Unlike conventional approaches to data uploading, the inventions described and claimed in the '399 Patent require synchronizing or other means of associating interactive and data transfer connections that, when used in combination with other claim elements, improve data uploading in unconventional ways. *See id*. For example, prior to the invention of the '399 Patent, existing data uploading methods included FTP file transfer that ran independently from a WWW session and had limited security, typing a file name into a java applet which is cumbersome because of the manual entry, or emailing files separately from the WWW connection. *See id.* at 1:20–27. The inventions described and claimed in the '399 Patent solved these problems and improved data uploading technology when implemented. *See, e.g., id*. at 1:41–3:47.

62. The solutions described and claimed in the '399 Patent represented a significant advance over existing approaches and were not well-known, routine, or conventional in the field at the time the application leading to the '399 Patent was filed. *See id*. at 1:41–3:47. During examination of the application that ultimately issued as the '399 Patent, the patent examiner at the USPTO considered multiple U.S. patent documents. *See id*. at Cover Page. These include references describing solutions from Oracle and ICTV, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the '399 Patent.

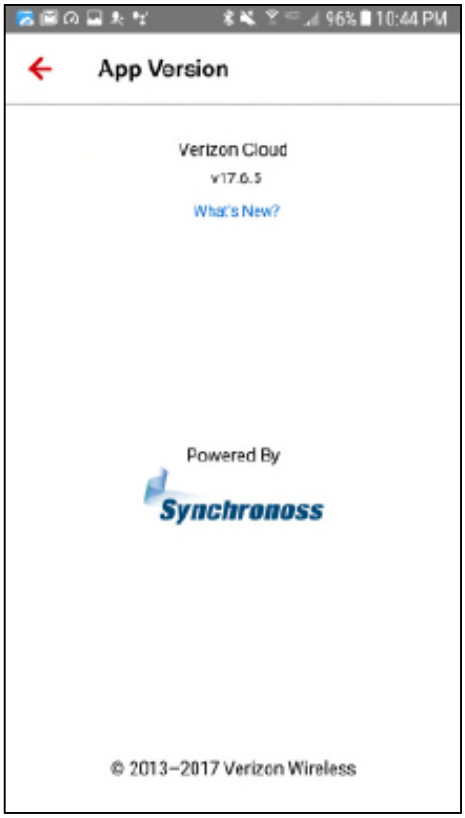
63. Synchronoss directly infringed one or more claims of the '399 Patent, either literally or under the doctrine of equivalents, by making, using, offering to sell, and selling the Synchronoss Personal Cloud. Non-limiting examples of such infringement are provided below, based on the information currently available to Dropbox.

64. Synchronoss's Personal Cloud product, for example, satisfies each and every limitation of Claim 25 of the '399 Patent.

65. Synchronoss's Personal Cloud is accessible via a mobile application, a desktop application running on a personal computer, and a website accessed using a web browser running on a personal computer.

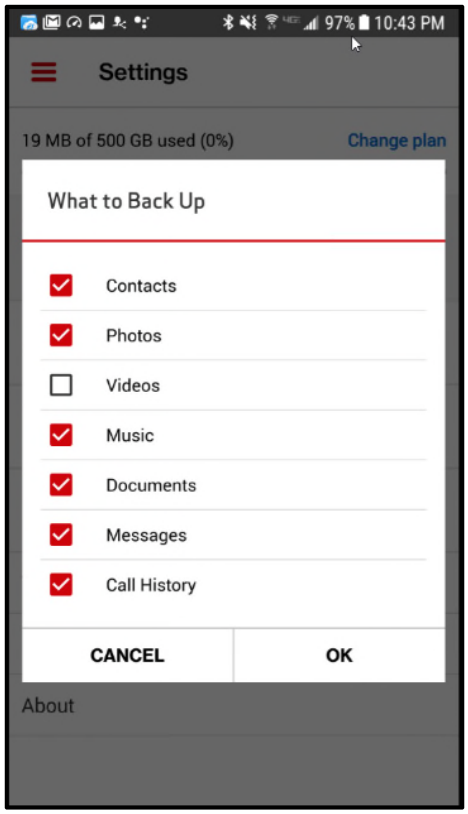
66. Synchronoss's Personal Cloud is an apparatus for uploading data files. For example, Synchronoss's Personal Cloud provides Personal Cloud to mobile network providers as a "white-label solution" for syncing, backing up, and uploading data (e.g., contacts, photographs, videos, music, documents, messages, and/or call history) stored on users mobile phones. *See* http://synchronoss.com/products/cloud/personal-cloud-solution.

67. For example, Synchronoss provides the Synchronoss Personal Cloud product to Verizon:



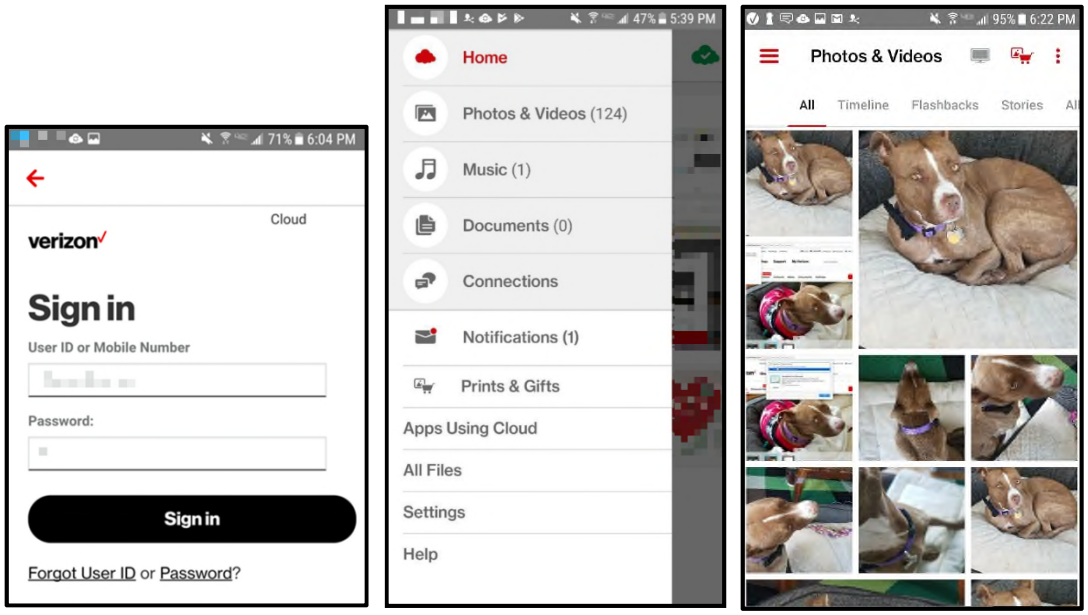
Synchronoss Personal Cloud mobile application screenshot.

68. Synchronoss's Personal Cloud includes a file upload connection server. For example, Synchronoss's Personal Cloud allows data, such as contacts, photographs, videos, music, documents, messages, and/or call history, to be uploaded to Synchronoss's Personal Cloud servers:



Synchronoss Personal Cloud mobile application screenshot.

69. Synchronoss's Personal Cloud includes an interactive connection server. For example, Synchronoss's Personal Cloud creates an interactive connection between user devices and Synchronoss's Personal Cloud servers allowing users to manage the transfer of data between their devices and Synchronoss's Personal Cloud servers. Synchronoss's Personal Cloud allows users to log into the Synchronoss Personal Cloud, browse files stored on the Synchronoss Personal Cloud servers, and sync and back up data files (e.g., contacts, photographs, videos, music, documents, messages, and/or call history).



Synchronoss Personal Cloud mobile application screenshot.

70. Synchronoss's Personal Cloud includes a synchronizer that synchronizes the operation of respective connections formed by the file upload connection server and by the interactive connection server. For example, the interactive and data transfer connections of Synchronoss's Personal Cloud are synchronized to achieve the backup, sync, restore, access, and share functionalities. Instructions for uploading files to Synchronoss's Personal Cloud servers are provided over an interactive connection. On information and belief, data files are selected for upload using an interactive connection and uploaded on a separate file upload connection, allowing users to continue interacting with Synchronoss's Personal Cloud while files are uploaded.

71. Synchronoss has been aware of Dropbox since at least March 27, 2015 when it filed a lawsuit against Dropbox.

72. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss investigated Dropbox's intellectual property before or during its lawsuit against Dropbox.

73. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss was aware of the '399 Patent prior to filing this complaint.

74. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss's infringement of the '399 Patent has been willful and deliberate.

75. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to conduct an investigation after learning of the '399 Patent.

76. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to take any remedial actions upon learning of the '399 Patent.

Count III – Infringement of U.S. Patent No. 6,178,505

77. Dropbox incorporates by reference the allegations in Paragraphs 1 through 76 above.

78. The '505 Patent was filed on March 4, 1998 and claims priority to U.S. provisional applications Nos. 60/039,542, filed March 10, 1997 and 60/040,262, filed March 10, 1997.

79. The Internet made accessing information easier and cheaper than ever before. With that increased access to information, however, came increased difficulty for those who sought to protect their information. Indeed, whenever a piece of information is accessible to a user via the Internet, it is potentially accessible to all users of the Internet. *See* Ex. C ('505 Patent) at 1:48–59. The Internet made it harder to protect information in at least two ways: (1) blocking intruders became a more-difficult technical problem, and (2) protecting information en route through the Internet became more difficult as it is impossible to ensure the security of each Internet switch a message passes through. *See id*. at 1:48–67. In addition, as internal networks grow and interconnect, "access-control issues characteristic of the Internet arise again—except this time with regard to internal access to data." *Id*. at 5:2–17.

80. Partial solutions to these problems existed in 1998, when the '505 Patent was filed, including the use of firewalls and tunneling using encryption. *Id.* at 2:45–47. If properly implemented, perimeter firewalls and encrypted tunneling could protect a network from external threats but did not address internal threats. A solution to internal security problems is to use internal firewalls to subdivide the internal networks, but this solution is not easily scaled. *Id.* at 4:5–21; 5:18–33.

81. To address these problems, the '505 Patent describes specific and discrete implementations that improved upon, and solved problems inherent in, prior art approaches to access filtering. The inventions described and claimed in the '505 Patent improved upon existing approaches by "providing only as much authentication and encryption security as is required for a given user, a given path through the network, and a given resource." *Id.* at 5:67–6:3. By identifying each user according to one or more modes of identification and granting access to an information resource only if the mode of identification is sufficiently trustworthy, a highly-scalable access filter was invented. *Id.* at 6:5–18. These advances were improvements over, and patentably distinct from, prior approaches to access filtering.

82. The '505 Patent describes and claims a number of novel and inventive approaches to access filtering, including providing only as much authentication and encryption security as is required for a given user, a given path through the network, and a given resource. These inventive approaches are captured in independent Claims 1, 16, and their respective dependent claims. The claimed approaches are tied to computers and cannot be performed by a human alone. Claim 1, for example, recites an "[a]pparatus that provides an information resource in response to a request from a user, the request including an identification of the user according to a mode of identification;" "access control information including a sensitivity level associated with the resource;" "a trust level associated with the mode of identification;" and "an access checker which permits the apparatus to provide the resource only if the trust level for the mode of identification is sufficient for the sensitivity level of the resource."

83. Claim 16 recites an "[a]pparatus that provides an information resource via a path through a network to a user in response to a request from the user," "access control information including a sensitivity level associated with the resource," "a path trust level associated with the path," "an encryption trust level associated with an encryption method" and "an access checker which permits the apparatus to provide the resource only if either the path trust level is sufficient for the sensitivity level or the encryption trust level is sufficient for the sensitivity level and the request is encrypted with the encryption method."

84. These claim elements, individually or in combination, are unconventional, and nothing in the specification describes these concepts as well-understood, routine, or conventional. To the contrary, as explained previously, the claimed concepts solve problems of the prior art described in the patent and provide advantages and improvements to access filtering that was unknown in the field before the invention of the '505 Patent. *See, e.g.*, Ex. C at 1:32–6:56. Unlike conventional approaches to access filtering, the inventions described and claimed in the '505 Patent require specific types of multi-factor authentication/access based on the mode of identification that, when used in combination with other claim elements, improve access filtering in unconventional ways. *See id*. For example, prior to the invention of the '505 Patent, existing access filtering methods, including firewalls and encrypted tunneling, did not address internal threats, and if applied to internal networks, did not easily scale. *See id*. at 2:45–47, 4:5–21; 5:2–33. The inventions described and claimed in the '505 Patent solved these problems and improved the security and scalability of access filtering when implemented. *Id*. at 1:32–6:56

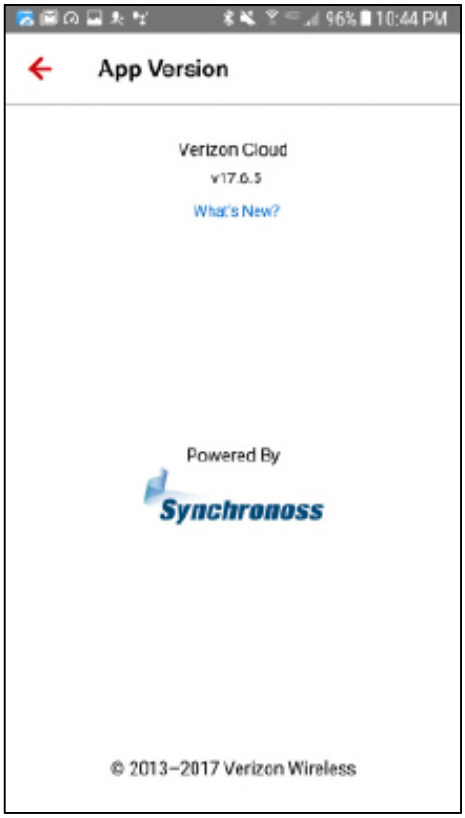
85. The solutions described and claimed in the '505 Patent represented a significant advance over existing approaches and were not well-known, routine, or conventional in the field at the time the application leading to the '505 Patent was filed. *See, e.g.*, Ex. C at 1:32–6:56. During examination of the application that ultimately issued as the '505 Patent, the patent examiner at the USPTO considered multiple U.S. patent documents. *See* Ex. C at Cover Page. These include references describing solutions from Secure Computing (now McAfee) and Check Point Software, amongst others. The patent examiner determined that none disclosed or rendered obvious the inventions of the '505 Patent.

86. Synchronoss directly infringed one or more claims of the '505 Patent, either literally or under the doctrine of equivalents, by making, using, offering to sell, and selling the Synchronoss Personal Cloud. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Dropbox.

87. Synchronoss's Personal Cloud, for example, satisfies each and every limitation of Claim 1 of the '505 Patent.

88. Synchronoss's Personal Cloud is accessible via a mobile application, a desktop application running on a personal computer, and a website accessed using a web browser running on a personal computer.

89. Synchronoss's Personal Cloud provides an information resource in response to a request from a user, the request including an identification of the user according to a mode of identification. For example, Synchronoss provides the Synchronoss Personal Cloud product to Verizon:



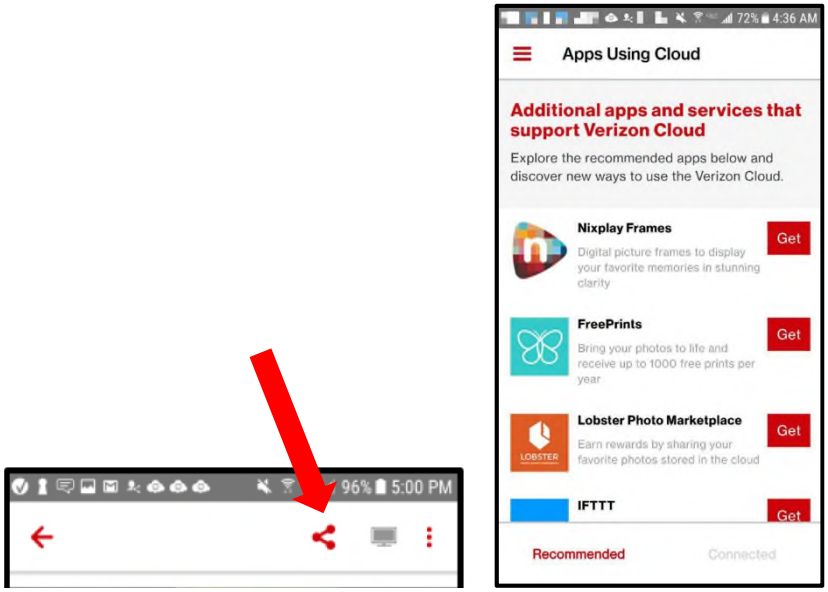
Synchronoss Personal Cloud mobile application screenshot.

90. Synchronoss's Personal Cloud requires a user to submit a login request in order to access information. A login request may include a user ID or a mobile number and an associated password, which uniquely identifies each user. In addition, Synchronoss's Personal Cloud uses additional information, such as device identifier, application identifier, information about the client hardware, information about the client software, and/or other user input to grant access to data in Synchronoss's Personal Cloud.

91. Synchronoss's Personal Cloud includes access control information including a sensitivity level associated with the resource. For example, Synchronoss's Personal Cloud includes at least three sensitivity levels for different information: (1) information that may be accessed by the owner, (2) information that may be accessed by the owner and a user with a shared link, and (3) information that may be accessed by the owner and a third-party application.

92. By default, information stored in Synchronoss's Personal Cloud may only be accessed by the owner.

93. Synchronoss's Personal Cloud provides a share functionality that permits a user to assign lower levels of sensitivity. Information can be shared by generating a direct link and/or by selecting third-party applications to share the information with:



Synchronoss Personal Cloud mobile application screenshots (annotated).

94. Synchronoss's Personal Cloud also includes access control information including a trust level associated with the mode of identification. For example, when a user logs in to access information stored in Synchronoss's Personal Cloud, Synchronoss's Personal Cloud utilizes a variety of information to determine what information may be accessed, including user ID, mobile number, password, device identifier, user input, application identifier, browser/operating system information, shared link, and/or encryption.

95. Synchronoss's Personal Cloud includes an access checker that permits the apparatus to provide the resource only if the trust level for the mode of identification is sufficient for the sensitivity level of the resource. For example, on information and belief, Synchronoss's Personal Cloud analyzes the information collected during login, and allows access to information based on the information collected during login. For example, if Synchronoss's Personal Cloud is being accessed from applications with insufficient security, only information shared via link may be accessed. Whereas, when Synchronoss's Personal Cloud is accessed using a user ID and password on a mobile application on carrier's network, all information in the user's Personal Cloud can be accessed.

96. Synchronoss has been aware of Dropbox since at least March 27, 2015 when it filed a lawsuit against Dropbox.

97. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss investigated Dropbox's intellectual property before or during its lawsuit against Dropbox.

98. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss was aware of the '505 Patent prior to filing this complaint.

99. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss's infringement of the '505 Patent has been willful and deliberate.

100. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to conduct an investigation after learning of the '505 Patent.

101. As will likely be shown after a reasonable opportunity for further investigation or discovery, Synchronoss failed to take any remedial actions upon learning of the '505 Patent.

PRAYER FOR RELIEF

WHEREFORE, Dropbox prays for judgment in its favor granting the following relief:

A. A finding that Synchronoss has infringed the patents Patents-in-Suit, either directly or indirectly by inducing others to infringe or contributing to infringement by others;

B. A finding that Synchronoss's infringement was willful and that Synchronoss's continued infringement is willful;

C. An award of damages pursuant to 35 U.S.C. § 284 adequate to compensate Dropbox for Synchronoss's infringement of the Patents-in-Suit, including both pre- and post-judgment interest and costs as fixed by the Court;

D. A preliminary and/or permanent injunction against Synchronoss and its officers, agents, servants, employees, and representatives, and all others in active concert or participation with them, from infringement of at least the '541 Patent.

E. A declaration that this is an exceptional case within the meaning of 35 U.S.C. § 285, and a corresponding award of Dropbox's reasonable attorney fees incurred in connection with the litigation; and

F. Any additional and further relief the Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b) and Northern District of California Civil Local Rule 3-6(a), Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 20, 2018

Respectfully submitted,

BAKER BOTTS L.L.P.

/s/ *Jeremy J. Taylor*
Jeremy J. Taylor

Attorney for Dropbox, Inc.

BAKER BOTTS L.L.P.
Wayne O. Stacy (SBN 314579)
wayne.stacy@bakerbotts.com
Sarah Guske (SBN 232467)

sarah.guske@bakerbotts.com
Jeremy J. Taylor (SBN 249075)
jeremy.taylor@bakerbotts.com
BAKER BOTTS L.L.P.
101 California Street, Suite 3600
San Francisco, California 94111
Telephone: (415) 291-6200
Facsimile: (415) 291-6300

Kurt M. Pankratz (*pro hac vice*)
kurt.pankratz@bakerbotts.com
BAKER BOTTS L.L.P.
2001 Ross Avenue
Dallas, Texas 75201-2980
Telephone: (214) 953-6584
Facsimile: (214) 661-4584

Jake W. Gallau (SBN 319656)
jake.gallau@bakerbotts.com
BAKER BOTTS L.L.P.
1001 Page Mill Road, Bldg. One, Suite 200
Palo Alto, California 94304
Telephone: (650) 739-7500
Facsimile: (650) 739-7699